

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-142682

(43)Date of publication of application : 25.05.2001

(51)Int.Cl.

G06F 7/58

(21)Application number : 11-323252

(71)Applicant : SONY CORP

(22)Date of filing : 12.11.1999

(72)Inventor : SHIBAIKE YUKO

NODA TOSHIHARU

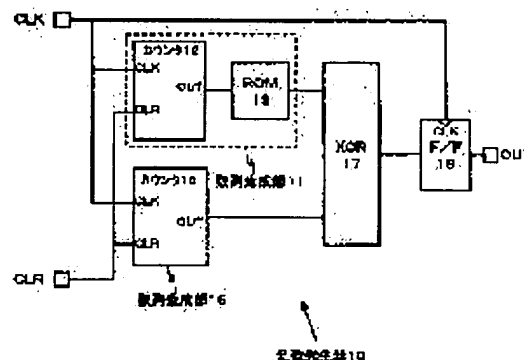
(54) RANDOM NUMBER GENERATOR AND RANDOM NUMBER GENERATING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To generate random numbers with long cycle at a low cost.

SOLUTION: This random number generator is provided with a first sequence generating part to generate a sequence with a first cycle, a second sequence generating part to generate a sequence with a second cycle and an arithmetic part to apply a prescribed arithmetic operation to the first and second sequences.

The first sequence generating part outputs random numbers read, for example, from a random number table. The second sequence generating part is allowed to be a counter output to increment in stepped or other complicated forms which are not the counter output other than a normal counter output. The arithmetic part generates uniform random numbers without deviation by applying XOR and XNOR, etc., to the first and second sequences. Since the generated random numbers have the greatest common divisor of the first and second cycles as the cycles, their cycles are easily prolonged.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-142682

(P2001-142682A)

(43) 公開日 平成13年5月25日(2001.5.25)

(51) Int. CL⁷

G 0 6 F 7/58

識別記号

F I

G 0 6 F 7/58

テ-マ-ド^{*}(参考)

A

審査請求 未請求 請求項の数12 O L (全 7 頁)

(21) 出願番号

特願平11-323252

(22) 出願日

平成11年11月12日(1999.11.12)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 芝池 優子

東京都品川区東五反田1丁目14番10号 株式会社ソニー木原研究所内

(72) 発明者 野田 俊治

東京都品川区東五反田1丁目14番10号 株式会社ソニー木原研究所内

(74) 代理人 100101801

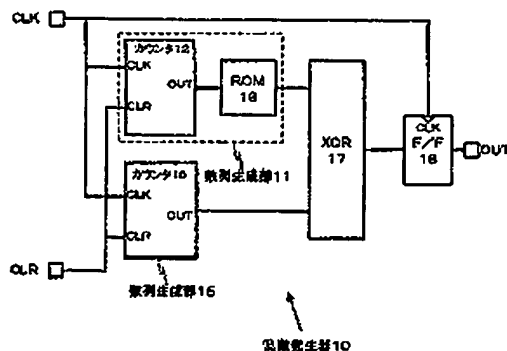
弁理士 山田 英治 (外2名)

(54) 【発明の名称】 乱数発生装置及び乱数発生方法

(57) 【要約】

【課題】 長周期の乱数を低コストで発生する。

【解決手段】 乱数発生装置は、第1の周期を持つ数列を生成する第1の数列生成部と、第2の周期を持つ数列を生成する第2の数列生成部と、前記第1及び第2の数列に対して所定の演算を適用する演算部とを備える。第1の数列生成部は例えば乱数テーブルから読み出した乱数を出力する。第2の数列生成部は通常のカウンタ出力である他、階段状その他複雑な形式でインクリメントするカウンタ出力、カウンタ出力でない数列でよい。演算部は、第1及び第2の数列にXORやXNORなどを適用して、偏りのない一様な乱数を生成する。生成された乱数は、第1及び第2の周期の最小公倍数を周期に持つので、容易に長周期化できる。



【特許請求の範囲】

【請求項1】第1の周期を持つ第1の数列を生成する第1の数列生成部と、

第2の周期を持つ第2の数列を生成する第2の数列生成部と、

前記第1及び第2の数列に対して所定の演算を適用する演算部と、

前記演算部の演算結果を乱数として出力する出力部と、を具備することを特徴とする乱数発生装置。

【請求項2】前記第1の数列生成部は、カウント値を逐次インクリメントするカウンタと、第1の周期を持つ乱数テーブルを含み、前記乱数テーブル中からカウンタ値に該当するエントリの乱数を出力することを特徴とする請求項1に記載の乱数発生装置。

【請求項3】前記第2の数列生成部は、 $0 \sim (N-1)$ の数値の範囲を逐次インクリメントし、周期 N を有するカウンタであることを特徴とする請求項1に記載の乱数発生装置（但し、 N は1以上の整数）。

【請求項4】前記第2の数列生成部は、 $0 \sim (N-1)$ の数値の範囲を階段状にインクリメントし、周期 $N \times (N+1)/2$ を有するカウンタであることを特徴とする請求項1に記載の乱数発生装置（但し、 N は1以上の整数）。

【請求項5】前記演算部は、前記第1及び第2の数列に対してXOR（排他的論理和）又はXNOR（排他的否定論理和）などの排他的論理演算を適用することを特徴とする請求項1に記載の乱数発生装置。

【請求項6】前記第1及び第2の周期は互いに約数を持たないことを特徴とする請求項1に記載の乱数発生装置。

【請求項7】第1の周期を持つ第1の数列を生成するステップと、

第2の周期を持つ第2の数列を生成するステップと、

前記第1及び第2の数列に対して所定の演算を適用するステップと、

前記演算部の演算結果を乱数として出力するステップと、を具備することを特徴とする乱数発生方法。

【請求項8】前記第1の数列を生成するステップでは、第1の周期を持つ乱数テーブル中から、逐次インクリメントされるカウンタ値に該当するエントリの乱数を出力することを特徴とする請求項7に記載の乱数発生方法。

【請求項9】前記第2の数列を生成するステップでは、 $0 \sim (N-1)$ の数値の範囲を逐次インクリメントして、周期 N を持つカウンタ値を生成することを特徴とする請求項7に記載の乱数発生方法（但し、 N は1以上の整数）。

【請求項10】前記第2の数列を生成するステップでは、 $0 \sim (N-1)$ の数値の範囲を階段状にインクリメントして、周期 $N \times (N+1)/2$ を有するカウンタ値を生成することを特徴とする請求項7に記載の乱数発生

方法（但し、 N は1以上の整数）。

【請求項11】前記所定の演算を適用するステップでは、前記第1及び第2の数列に対してXOR（排他的論理和）又はXNOR（排他的否定論理和）などの排他的論理演算を適用することを特徴とする請求項7に記載の乱数発生方法。

【請求項12】前記第1及び第2の周期は互いに約数を持たないことを特徴とする請求項7に記載の乱数発生方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、無作為に選ばれた全く不規則な数字の列で構成される乱数を発生するための乱数発生装置及び乱数発生方法に係り、特に、長周期の乱数を発生することができる乱数発生装置及び乱数発生方法に関する。

【0002】

【従来の技術】昨今の情報処理技術の進歩に伴い、各種のコンピュータ・システムが広汎に普及してきている。コンピュータ上では、テキスト、画像、音声などある種のデータをデジタル化して、各種の業務処理の支援・自動化が可能である。

【0003】かかるコンピュータ処理の各局面においては、乱数、すなわち無作為に選ばれた全く不規則で偏りのない数字の列がしばしば利用される。例えば、データの暗号化や電子認証を行う際などに、各数値の間に相関性がなく、第3音が予測しにくい乱数を使用する。また、各種の自然現象や経済現象などのシミュレーションを行う場合その他、人為的でなく自然で一様な塊の数字を必要とする場合にも、乱数が用いられる。また、映像シーンの切り替えなどを行う映像処理装置においては、ランダムな色配列の連続画像を生成するために、乱数を適用することもある。

【0004】図1には、一般的な乱数発生器20の構成例を模式的に図解している。この乱数発生器20は、カウンタ21と、あらかじめ乱数テーブルを格納したROM（Read Only Memory）22と、フリップ・フロップ23とで構成される。すなわち、カウンタ21は、クロック信号の入力に反応して逐次インクリメントされるカウンタ値を出力し、ROM22は入力されたカウンタ値に該当するテーブル・エントリの乱数を出力し、フリップ・フロップ23は、クロック信号に同期して乱数を外部出力するようになっている。ROM22に格納される乱数テーブルは、例えばM系列（maximal-period sequence）乱数など各種の乱数発生方式等を用いて作成される。

【0005】既に図知のように、乱数は、数字の列が不規則すなわち統計的精度で偏りがなく一様性が充分保たれていることが好ましい。また、乱数は、再び同じ数字の列が繰り返されるようになるまでの周期が長いことが

好ましいとされている。

【0006】ところが、図1に示すような構成の乱数発生器20の場合、ROM22に格納されている乱数の個数が最終的に得られる乱数の周期となってしまう。したがって、長周期の乱数を得たい場合には、ROM22すなわち乱数テーブルの容量を大きくしなければならないことになり、コスト増大を招来してしまう。

【0007】一般に、8ビットのM系列乱数を発生するハードウェア装置は、1ビットのシフト・レジスタを8個と、原始多項式に基づく演算を行うための排他的論理和装置(XOR)とで構成される(図示しない)。M系列乱数によって生成される8ビットの疑似乱数の周期は、理論上、 $2^8 - 1 = 255$ となる。シフト・レジスタの個数を増やして周期を長くした場合、8ビットの疑似乱数を得るためにビット・マスクを施すと乱数性が失われるので、有効ではない。

【0008】

【発明が解決しようとする課題】本発明の目的は、無作為に選ばれた全く不規則な数字の列で構成される乱数を発生することができる、優れた乱数発生装置及び乱数発生方法を提供することにある。

【0009】本発明の更なる目的は、長周期の乱数を低コストで発生することができる、優れた乱数発生装置及び乱数発生方法を提供することにある。

【0010】

【課題を解決するための手段】本発明は、上記課題を参照してなされたものであり、その第1の側面は、第1の周期を持つ数列を生成する第1の数列生成部と、第2の周期を持つ数列を生成する第2の数列生成部と、前記第1及び第2の数列に対して所定の演算を適用する演算部と、前記演算部の演算結果を乱数として出力する出力部と、を具備することを特徴とする乱数発生装置である。

【0011】前記第1の数列生成部は、カウンタ値を逐次インクリメントするカウンタと、第1の周期を持つ乱数テーブルを含み、前記乱数テーブルの中からカウンタ値に該当するエントリの乱数を出力するようにしてもよい。

【0012】また、前記第2の数列生成部は、 $0 \sim (N-1)$ の数値の範囲を逐次インクリメントし、周期Nを有するカウンタであってもよい。あるいは、第2の数列生成部は、 $0 \sim (N-1)$ の数値の範囲を階段状にインクリメントし、周期 $N \times (N+1) / 2$ を有するカウンタであってもよい。

【0013】また、前記演算部は、前記第1及び第2の数列に対してXOR(排他的論理和)又はXNOR(排他的否定論理和)などの排他的論理演算を適用してもよい。排他的演算を施すことにより、出力が0又は1の一方に偏ることがなく、元の乱数の一様性を維持することができる。

【0014】また、前記第1及び第2の周期は互いに約

数を持たないような値に設定することによって、長周期化の効果を高めることができる。

【0015】また、本発明の第2の側面は、第1の周期を持つ第1の数列を生成するステップと、第2の周期を持つ第2の数列を生成するステップと、前記第1及び第2の数列に対して所定の演算を適用するステップと、前記演算部の演算結果を乱数として出力するステップと、を具備することを特徴とする乱数発生方法である。

【0016】前記第1の数列を生成するステップでは、第1の周期を持つ乱数テーブルの中から、逐次インクリメントされるカウンタ値に該当するエントリの乱数を出力するようにしてもよい。

【0017】また、前記第2の数列を生成するステップでは、 $0 \sim (N-1)$ の数値の範囲を逐次インクリメントして、周期Nを持つカウンタ値を生成するようにしてもよい。あるいは、第2の数列を生成するステップでは、 $0 \sim (N-1)$ の数値の範囲を階段状にインクリメントして、周期 $N \times (N+1) / 2$ を有するカウンタ値を生成するようにしてもよい。

【0018】また、前記所定の演算を適用するステップでは、前記第1及び第2の数列に対してXOR(排他的論理和)又はXNOR(排他的否定論理和)などの排他的論理演算を適用するようにしてもよい。排他的演算を施すことにより、出力が0又は1の一方に偏ることがなく、元の乱数の一様性を維持することができる。

【0019】また、前記第1及び第2の周期は互いに約数を持たないような値に設定することによって、長周期化の効果を高めることができる。

【0020】

【作用】本発明に係る乱数発生装置は、第1の周期を持つ数列を生成する第1の数列生成部と、第2の周期を持つ数列を生成する第2の数列生成部と、前記第1及び第2の数列に対して所定の演算を適用する演算部とを備えている。

【0021】第1の数列生成部は、例えば、乱数テーブルから読み出した乱数を出力する。また、第2の数列生成部は、通常のカウンタ出力である他、階段状その他複雑な形式でインクリメントするカウンタ出力、カウンタ出力でない数列などを出力する。

【0022】演算部は、第1及び第2の数列に対してXOR(排他的論理和)やXNOR(排他的否定論理和)などの排他的論理演算を適用して、偏りのない一様な乱数を生成することができる。

【0023】生成された乱数は、第1及び第2の周期の最小公倍数を周期に持つので、容易に長周期化できる。

【0024】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0025】

【発明の実施の形態】以下、図面を参照しながら本発明

の実施例を詳解する。

【0026】図2には、本発明を實現した乱数発生器10の構成を模式的に示している。同図に示すように、乱数発生器10は、クロック信号にตอบสนองして逐次的に数列を出力する第1及び第2の数列生成部11、15と、各数列生成部11及び15の出力に対して所定の演算処理を適用する演算部17と、該演算出力をクロックに同期して外部出力するフリップ・フロップ18とで構成される。

【0027】数列生成部11及び15は、それぞれJ及びKという周期で数列を生成するものとする。数列生成部11又は15のうちいずれか一方は、その出力自体が不規則で一様性のある乱数であることが好ましい。また、数列生成部11又は15の他方は、カウンタの出力*

*又はカウンタ値に基づいた出力であってもよい。

【0028】演算部17は、数列生成部11及び15の出力同士に所定の論理演算を適用する機能モジュールである。ここで言う論理演算は、ANDやORではなく、XOR（排他的論理和）やXNOR（排他的否定論理和）のような排他的論理演算であることが好ましい。これは、ANDでは出力が0に偏り、ORでは出力が1に偏るのに対して、XORやXNORなどの排他的論理演算によれば、出力に偏りがなくなるからである（表1を参照のこと）。すなわち、乱数に対してこのような排他的演算を適用しても、元の乱数の一様性は失われない。

【0029】

【表1】

入力	AND	OR	XOR	XNOR
0	0	0	0	1
0	1	0	1	0
1	0	1	0	1
1	1	1	1	0

【0030】演算部17の出力、すなわち、この乱数発生器10が出力する乱数は、各数列生成部11及び15が持つ周期J、Kの最小公倍数となる。したがって、周期J及びKを適切な値に設定することにより、比較的短い周期Jしか持たない乱数を基にして、最長でJ×Kという長周期を持つ乱数を生成することができる。

【0031】図3には、本発明を實現した乱数発生器10の他の構成例を図解している。同図に示す例では、数列生成部11は、カウンタ12とROM（Read Only Memory）13によって構成され、数列生成部15は、カウンタ16によって構成される。また、演算部17は、XOR（排他的論理和）によって構成される。

【0032】カウンタ12は、クロック信号の入力にตอบสนองして逐次インクリメントされるカウント値をROM13に供給する。ROM13には、あらかじめ乱数テーブルが格納されており、入力されたカウント値に該当するテーブル・エントリの乱数を出力するようになっている。乱数テーブルは、例えば、M系列（maximal period sequence）乱数など各種の乱数発生方式等を用いて作成することができる。

【0033】この例では、ROM13には、2進数8ビットの値をとる乱数256個からなる乱数テーブルが格納されており、言い換えれば、数列生成部11の周期は256である。

【0034】なお、ROM13は、1チップ構成のメモリとして、乱数発生器10に対して着脱・交換可能に構成することで、乱数テーブルを容易に更新することができる。あるいは、EEPROM（Electrically Erasable and Programmable Memory）（以下、

ble ROM）のような消去書き込み可能なメモリをROM13に採用することによっても、乱数テーブルをプログラマブルにすることができる。

【0035】また、カウンタ16は、クロック信号の入力にตอบสนองして逐次インクリメントされるカウンタ値を基に、所定の数列を出力するように構成されている。

【0036】乱数発生器10を長周期化するという要請から、カウンタ16の周期は、数列生成部11の周期256との最小公倍数が大きくなる値に設定することが好ましい。この例では、カウンタ16は、0から249までの値を0、1、0、1、2、0、1、2、3、0、1、2、3、…、0、1、2、…、249という具合に階段状にカウントしていくものとする。この場合のカウンタ16の周期は $256 \times 251 / 2$ となる。したがって、乱数発生器10全体の周期は $256 \times 250 \times 251 / 2 (= 8,032,000)$ となり、数列生成部11単体の乱数が持つ周期よりもはるかに長期化することができる。

【0037】図3に示すような構成によれば、カウンタ16やROM13の容量を変えることによって、用途に応じて充分な長さの周期を持つ乱数を発生させることができる。

【0038】乱数発生器10の最終的な周期は、ROM13すなわち乱数テーブルの容量とカウンタ16の周期との最小公倍数となる。したがって、カウンタ16の周期を、乱数の個数との約数のない値に設定することによって、長周期化の効果が高くなる。

【0039】上述した例では、ROM13内の乱数の個数すなわち周期が256の場合に、カウンタ16を0～249の間の値を階段状にカウントする構成にして、そ

の周期は $250 \times 251 / 2$ となる。その他、カウンタ16を0~245, 0~248, 0~253の各値の間で階段状にカウントする場合であっても、周期はそれぞれ $246 \times 247 / 2$, $249 \times 250 / 2$, $254 \times 255 / 2$ となり、256とは約数がないので、長周期化の効率が低い。

【0040】また、所望の周期の長さやコスト、ハードウェア設計上の制約などにより、カウンタ16を、通常のカウンタ、上記よりもさらに複雑な階段状のカウント方式、あるいは、カウンタ以外の数列生成などの中から適宜選択することができる。

【0041】上述の実施例では、図2及び図3に示すような専用のハードウェア装置を用いて乱数を発生する。勿論、プログラミング言語で記述されたコンピュータ・ソフトウェアなどを用いた所定の処理手順に従って、同様の乱数発生方式を実現することも可能である。

【0042】図4には、本発明に係る乱数発生方式を実現するための処理手順をフローチャートの形式で図解している。以下、各ステップについて説明する。

【0043】まず、ステップS11では、所定の周期Jを持つ第1の数列を生成する。第1の数列は、それ自体が不規則で一様性のある乱数であることが好ましい。

【0044】次いで、ステップS12では、所定の周期Kを持つ第2の数列を生成する。第2の数列は、例えば、通常のカウンタの出力である他、階段状など複雑なインクリメントを行うカウンタ出力、あるいは、カウンタ出力ではない数列であってもよい。

【0045】次いで、ステップS13では、第1及び第2の数列同士に対して所定の演算を適用する。ここで言う演算は、論理演算を意味し、とりわけXOR（排他的論理和）やXNOR（排他的否定論理和）などの排他的論理演算であることが好ましい。これは、ANDでは出力が0に偏り、ORでは出力が1に偏るのに対して、XORやXNORなどの排他的論理演算によれば、出力に偏りがなくなるからである（前述及び〔表1〕を参照のこと）。

【0046】最後に、ステップS14において、上記の演算結果を乱数として出力して、この処理全体を終了する。

【0047】上述した処理手順に従って生成される乱数は、第1及び第2の数列の各々が持つ周期J、Kの最小公倍数となる。したがって、周期J及びKを適切な値に設定することにより、比較的短い周期Jしか持たない乱数を基にして、最大J×Kの長周期を持つ乱数を生成することができる。

【0048】図5には、本発明に係る乱数発生方式を実現するための処理手順の他の例をフローチャートの形式で図解している。以下、各ステップについて説明する。

【0049】まず、ステップS21では、カウンタ値を出力し、次いでステップS22では、所定の周期Jを持つ

乱数テーブルの中からカウンタ値に該当するエントリから乱数を取り出す。乱数テーブルは、例えば、M系列（maximal-period sequence）乱数など各種の乱数発生方式等を用いて作成することができる。

【0050】次いで、ステップS23では、所定の周期Kを持つ数列を生成する。この数列は、例えば、通常のカウンタの出力である他、階段状など複雑なインクリメントを行うカウンタ出力、あるいは、カウンタ出力ではない数列であってもよい。

【0051】次いで、ステップS24では、ステップS22で得られた乱数とステップS23で生成された数列を各入力として、所定の演算を適用する。ここで言う演算は、論理演算を意味し、とりわけXOR（排他的論理和）やXNOR（排他的否定論理和）などの排他的論理演算であることが好ましい。これは、ANDでは出力が0に偏り、ORでは出力が1に偏るのに対して、XORやXNORなどの排他的論理演算によれば、出力に偏りがなくなるからである（前述及び〔表1〕を参照のこと）。

【0052】最後に、ステップS25において、演算結果を乱数として出力して、この処理全体を終了する。

【0053】上述した処理手順に従って生成される乱数は、第1及び第2の数列の各々が持つ周期J、Kの最小公倍数となる。したがって、周期J及びKを適切な値に設定することにより、比較的短い周期Jしか持たない乱数を基にして、最大J×Kの長周期を持つ乱数を生成することができる。

【0054】〔追補〕以上、特定の実施例を参照しながら、本発明について詳述してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参照すべきである。

【0055】

【発明の効果】以上詳記したように、本発明によれば、無作為に選ばれた全く不規則な数字の列で構成される乱数を発生することができる。優れた乱数発生装置及び乱数発生方法を提供することができる。

【0056】また、本発明によれば、長周期の乱数を低コストで発生することができる。優れた乱数発生装置及び乱数発生方法を提供することができる。

【0057】本発明に係る乱数発生装置及び乱数発生方法によれば、ほぼ一様で偏りのない乱数を発生することができる。

【0058】本発明に従って発生した乱数を、例えば、トレイル（trail）などのシーン切り替え効果を行う映像処理装置に適用した場合には、色配列が美しい画

像を生成することができる。また、乱数の周期が非常に長いので、生成した画像を連続画像として見た際にも、視聴者は画像の繰り返しに気付くことがない。

【0059】本発明に係る乱数発生装置によれば、ROM13に格納する乱数テーブルを書き換える、又は、別の乱数テーブルを持ったROM13に交換することによって、異なる乱数を容易に生成することができる。また、ROM13内の乱数の周期や、カウンタ16の周期を切り替えることによって、様々な周期の乱数を生成することができる。

【0060】また、本発明に係る乱数発生装置は、従来方式に比し、コスト面、ハードウェア設計の面でも優れている。

【図面の簡単な説明】

【図1】一般的な乱数発生器20の構成例（従来例）を模式的に示した図である。

【図2】本発明を實現した乱数発生器10の構成を模式*

*的に示した図である。

【図3】本発明を實現した乱数発生器10の他の構成例を模式的に示した図である。

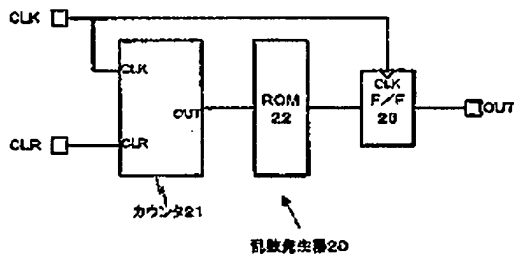
【図4】本発明に係る乱数発生方式を実現するための処理手順を示したフローチャートである。

【図5】本発明に係る乱数発生方式を実現するための処理手順の他の例を示したフローチャートである。

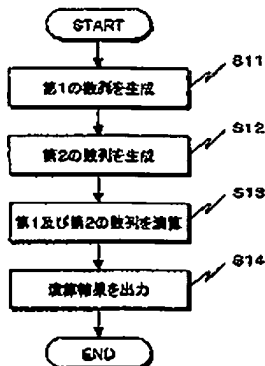
【符号の説明】

- 10…乱数発生装置
- 11…数列生成部
- 12…カウンタ
- 13…ROM（乱数テーブル）
- 15…数列生成部
- 16…カウンタ
- 17…演算部
- 18…フリップ・フロップ

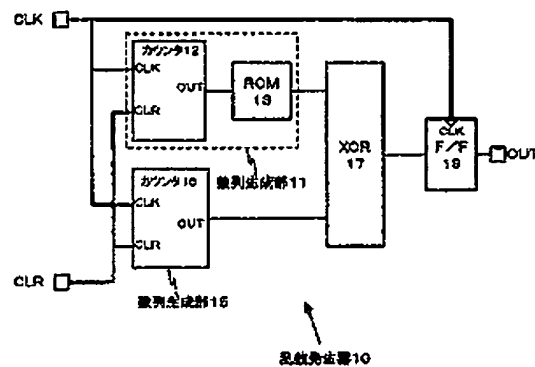
【図1】



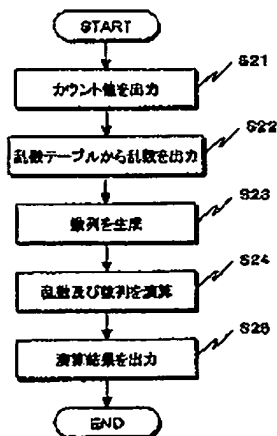
【図4】



【図3】



【図5】



[図2]

